



defined a split mask value

Search Patents

Advanced Patent Search

## Patents

Patents 1 - 10 on obtaining the key and random key mask value. (0.09 seconds)

## › List view

[Cover view](#)

## › Sort by relevance

[Sort by date \(new first\)](#)[Sort by date \(old first\)](#)

## › Any status

[Issued patents](#)[Applications](#)**[APPLICATION]** Security countermeasures for power analysis attacks

US Pat. 10825291 - Filed Apr 16, 2004

plaintext **value** using a look up on a table, the method comprising the following steps; a) **obtaining the key** and a **random value** *r*; b) **obtaining** a set of *n* ...**[APPLICATION]** Method of using a **mask** programmed **key** to securely configure a field ...

US Pat. 7240218 - Filed Feb 8, 2001 - Algotronix, Ltd.

The use of cipher block chaining and a **random** initial **value** makes cryptanalysis based ... Attack 6 is probably the most cost effective way of **obtaining key** ...**[APPLICATION]** Encryption secured against DPA

US Pat. 10028265 - Filed Dec 28, 2001 - FUJITSU LIMITED

... thereby **obtain** effects similar to the conventional **random mask value** method, while the conventional method **masks** an input or a **key** using **random values**. ...**[APPLICATION]** Key masking for cryptographic processes

US Pat. 11126208 - Filed May 13, 2005 - Research In Motion Limited

... **key value** into a set of split **key values**, b) defining a set of **random mask values**, c) combining multiple **random mask values** to define non-uniform **key** ...**[APPLICATION]** Secure caching technique for shared distributed caches

US Pat. 11347860 - Filed Feb 6, 2006 - International Business Machines Corporation

In step S6, the encrypted **mask value** *M* is decrypted using the secret **key** *SK*. ... [0032] In step S34, a **random mask value** *M* is generated and retained, ...**[APPLICATION]** Key agreement system, shared-key generation apparatus, and shared-key ...

US Pat. 10725102 - Filed Dec 2, 2003

[0538] Next, the shared-**key** encryption unit 118 receives a plurality of plaintexts *mi* ( $1 \leq i \leq n$ ) from a ... [0544] The **random**-number **mask** removal unit ...**[APPLICATION]** Access control apparatus, access control system, processor, access control ...

US Pat. 11523003 - Filed Sep 19, 2006

For example, a **value** generated from the cryptic **key** by using a hash function can be used as ... the **value** of the **random** number for **mask** is superposed by an ...**Method and system for providing secure key distribution in a communication** ...

US Pat. 5729608 - Filed Jan 24, 1996 - International Business Machines Corp.

A **key** being distributed must be a **random**, unpredictable quantity. ... The adversary can try to **obtain** the **MASK** value by interrogating B and pretending to be ...**Digital radio transceiver with encrypted key storage**

US Pat. 5481610 - Filed Feb 28, 1994 - Ericsson Inc.

13 14 **value** is transferred to the radio microcomputer 58 via **key** load cable 102 (block 208). ... 58 to re-randomize the **random value** stored within table 78. ...

Google ►  
1 2 3 4 5 6 7 8 9 10 Next

---

obtaining the key and random key mask value Search Patents

[Advanced Patent Search](#)

---

[Google Home](#) - [About Google](#) - [About Google Patents](#) - [Google Patents Help](#)

©2010 Google